UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,847	08/06/2001	Maclen Marvit	53635-0505	2160

29989 7590 06/16/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/923,847	MARVIT ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *05312005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-66 are pending for examination.

2. Claims 1-66 are rejected.

Specification

The disclosure is objected to because of the following informalities: the specification page 1, line 4 is missing the associated patent number (6,625,734) for the related application 09/300,085 .

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-17,20-22,25-27,30-33,36-39,42-45,48-51,55-57,61-63 are rejected under 35 U.S.C. 102(b) as being anticipated by Matsumoto, U.S. Patent 6,215,877 B1.

4. As per claim 1; "A method for controlling and tracking access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

receiving a request from the first node for

a message identifier that uniquely identifies the message and

a key that may be used to encode the message *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys for the subsequent data transfer (i.e., the chat content data), as a result of requesting to establish a chat channel (i.e., inherently an identification or identifier embedded in the key request), clearly encompasses the "...receiving a request ... uniquely identifies ... key ... encode the message ...", as broadly interpreted by the examiner.]*;

generating, in response to the request, both

the message identifier and

the key *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys (i.e., inherently generated per se in order to have been transferred) for the subsequent data transfer (i.e., the chat content data), as a result of requesting to establish a chat channel (i.e., inherently an identification or identifier embedded in the key request), clearly encompasses the "...generating ... request ... identifier ... key ...", as broadly interpreted by the examiner.]*;

providing both

the message identifier and

the key to

the first node to allow the message to

be encoded with the key to generate an encoded message

[figures 4-7 and associated descriptions, whereas the individual

chat clients on the chat network receiving secret keys (i.e., inherently generated per se in order to have been transferred) for the subsequent data transfer (i.e., the chat content data), as a result of requesting to establish a chat channel (i.e., inherently an identification or identifier embedded in the key request), clearly encompasses the "...providing both ... identifier ... key ...", as broadly interpreted by the examiner.];

receiving a request from the second node for

the key *[figures 4-7 and associated descriptions, whereas the individual chat clients (i.e., both the initiating (initially a sending or encoding side) and 2nd participating chat client (initially a receiving or decoding side)) on the chat network receiving secret keys for the subsequent data transfer, as a result of requesting to establish a chat channel, clearly encompasses the "...request ... second node ... key ...", as broadly interpreted by the examiner.]*;

generating algorithm identification data that

indicates an algorithm to be used to decode the encoded message *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network having had received secret keys for the subsequent data transfer, such that the encoding/decoding can properly occur, is inherently an indication that encoding/decoding are using the same algorithm (i.e., they use the same or in the case of a PKI configuration, the associated public/private key pair), clearly*

encompasses the "...algorithm ... decode the encoded message ...", as broadly interpreted by the examiner.];

providing the algorithm identification data to

the second node *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network having had received secret keys for the subsequent data transfer, such that the encoding/decoding can properly occur, is inherently an indication that encoding/decoding were provided the same algorithm, clearly encompasses the "...providing ... identification data ... second node ...", as broadly interpreted by the examiner.]*;

providing

the key and

the identification data to

the second node to allow

the encoded message to be decoded and

the message to be retrieved using the key *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network having had received secret keys for the subsequent data transfer, such that the encoding/decoding can properly occur, is inherently an indication that encoding/decoding were provided the same ID, key, etc., clearly encompasses the "...providing ... key ... identification data ... second node ... encoded message to*

be decoded ... message to be retrieved ...", as broadly interpreted by the examiner.]; and

deleting the key based upon

specified key policy criteria to

prevent copies of the encoded message from being decoded

[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys, subsequently transferring data, and the channel status monitor section (i.e., figure 7) generating another replacement secret key (i.e., inherently deleting the effective chat data transfer key, in of itself a function of a policy per se that is an operational characteristic of the chat system), clearly encompasses the "...deleting the key ... specified key policy ... prevent copies ... decoded", as broadly interpreted by the examiner.].".

Further, as per claim 6, this claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, as such; "A computer-readable medium carrying one or more sequences of one or more instructions for controlling and tracking access to a message that is communicated from a first node to a second node in a network, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of

receiving a request from the first node for a message identifier that uniquely identifies the message and a key that may be used to encode the message;

generating, in response to the request, both the message identifier and the key;

providing both the message identifier and the key to the first node to allow the message to be encoded with the key to generate an encoded message;

receiving a request from the second node for the key;

generating algorithm identification data that indicates an algorithm to be used to decode the encoded message;

providing the algorithm identification data to the second node;

providing the key and the identification data to the second node to allow the encoded message to be decoded and the message to be retrieved using the key; and

deleting the key based upon specified key policy criteria to prevent copies of the encoded message from being decoded.".

5. Claim 2 ***additionally recites*** the limitation that; "The method as recited in Claim 1, further comprising:

receiving a second request from the first node for

a second message identifier that uniquely identifies a second message and

a second key that may be used to encode the second message;

generating, in response to the second request, both

the second message identifier and

the second key;

providing both

the second message identifier and

the second key to

the first node to allow the second message to

be encoded with the second key to generate a second

encoded message;

receiving a second request from the second node for

the second key;

generating second algorithm identification data that

indicates a second algorithm to be used to decode the second encoded

message;

providing the second algorithm identification data to

the second node;

providing

the second key and

the second identification data to

the second node to allow

the second encoded message to be decoded and

the second message to be retrieved using the second key;

and

deleting the second key based upon

the specified key policy criteria to

prevent copies of the second encoded message from being decoded.".

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the inherent packet assembly/disassembly and associated transfer, and associated routing (Internet stack and flow control, and via Web links) nature of the Internet (i.e., packets consisting of data fragments), clearly encompasses the multiple packets per chat session/multiple sessions per chat (i.e., full duplex communications, whereas this claim is the multiple packet or iterative communications case of claim 1) elements of the claim language, as broadly interpreted by the examiner.).

Further, as per claim 7, this claim is the embodied software claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection, as such; "The computer-readable medium as recited in Claim 6, wherein the one or more sequences of one or more instructions include one or more additional sequences of one or more additional instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving a second request from the first node for a second message identifier that uniquely identifies a second message and a second key that may be used to encode the second message;

generating, in response to the second request, both the second message identifier and the second key;

providing both the second message identifier and the second key to the first node to allow the second message to be encoded with the second key to generate a second encoded message;

receiving a second request from the second node for the second key;

generating second algorithm identification data that indicates a second algorithm to be used to decode the second encoded message;

providing the second algorithm identification data to the second node;

providing the second key and the second identification data to the second node to allow the second encoded message to be decoded and the second message to be retrieved using the second key; and

deleting the second key based upon the specified key policy criteria to prevent copies of the second encoded message from being decoded.".

Further, as per claim 11, this claim is the apparatus claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection, as such; "A computer system for controlling and tracking access to a message that is communicated from a first node to a second node in a network comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

receiving a second request from the first node for a second message identifier that uniquely identifies a second message and a second key that may be used to encode the second message;

generating, in response to the second request, both the second message identifier and the second key;

providing both the second message identifier and the second key to the first node to allow the second message to be encoded with the second key to generate a second encoded message;

receiving a second request from the second node for the second key;

generating second algorithm identification data that indicates a second algorithm to be used to decode the second encoded message;

providing the second algorithm identification data to the second node;

providing the second key and the second identification data to the second node to allow the second encoded message to be decoded and the second message to be retrieved using the second key; and

deleting the second key based upon the specified key policy criteria to prevent copies of the second encoded message from being decoded.".

6. Claim 3 ***additionally recites*** the limitation that; "The method as recited in Claim 1, wherein

the decoding identification data further indicates

a location wherein the algorithm can be found."

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network having had received secret keys for the subsequent data transfer, such that the encoding/decoding can properly occur, is inherently an indication that encoding/decoding were provided the same ID, key, etc., and were communicated across the network to the appropriate node address (i.e., identification of location), clearly encompasses the "... decoding identification ... location ... algorithm can be found ...", as broadly interpreted by the examiner.).

Further, as per claim 8, this claim is the embodied software claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection, as such; "The computer-readable medium as recited in Claim 6, wherein the decoding identification data further indicates a location wherein the algorithm can be found.".

Further, as per claim 13, this claim is the apparatus claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection, as such; "The computer system as recited in Claim 11, wherein the decoding identification data further indicates a location wherein the algorithm can be found.".

7. Claim 4 ***additionally recites*** the limitation that; "The method as recited in Claim 1, wherein

the algorithm identification data is

generated at the first node."

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network having had received secret keys for the subsequent data transfer, such that the encoding/decoding can properly occur, is inherently an indication that encoding/decoding were provided the same ID, key, etc., (i.e., since the originating chat node subsequently communicates with the 2nd chat node, the encoding/decoding algorithm identification information inherently is passed from node 1 to node 2) and were communicated across the network to the appropriate node address (i.e., identification of location), clearly encompasses the "...algorithm identification ... generated ... first node", as broadly interpreted by the examiner.).

Further, as per claim 9, this claim is the embodied software claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection, as such; "The computer-readable medium as recited in Claim 6, wherein the algorithm identification data is generated at the first node.".

Further, as per claim 14, this claim is the apparatus claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection, as such; "The computer system as recited in Claim 11, wherein the algorithm identification data is generated at the first node.".

8. Claim 5 ***additionally recites*** the limitation that; "The method as recited in Claim 1, wherein

the algorithm identification data is

stored at a key repository."

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network having had received secret keys (i.e., via the key management server functions, in of itself clearly a key repository) for the subsequent data transfer, such that the encoding/decoding can properly occur, and were communicated across the network to the appropriate node address (i.e., identification of location), clearly encompasses the "...algorithm identification ... stored ... repository", as broadly interpreted by the examiner.).

Further, as per claim 10, this claim is the embodied software claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection, as such; "The computer-readable medium as recited in Claim 6, wherein the algorithm identification data is stored at a key repository.".

Further, as per claim 15, this claim is the apparatus claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection, as such; "The computer system as recited in Claim 11, wherein the algorithm identification data is stored at a key repository.".

9. As per claim 16, this claim is the broader claim in that the encoded message does not, at the very least, first require an identifier from the second node prior to encoding, as specifically

designated from originating at the second node for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, as such; "A method for controlling access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

generating, at the first node,

an encoded message by encoding the message with a key *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys (i.e., inherently generated per se in order to have been transferred) for the subsequent data transfer (i.e., the chat content data, post message encoding), as a result of requesting to establish a chat channel, clearly encompasses the "... generating ... first node ... encoded message ... key ...", as broadly interpreted by the examiner.]*;

generating, at the first node,

a set of one or more instructions that contain

the encoded message and

instructions for decoding the encoded message using the key *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys (i.e., inherently generated and identified as part of the 2 chat participating nodes identity per se in order to have been transferred) for the subsequent data transfer (i.e., the chat content data, post message encoding), as a result of requesting to establish a chat channel, and, whereas the key generation knows to 'whom' it must establish a decoding key (i.e., the 1st chat participant identity must be made known to the key generating element), clearly*

encompasses the "... generating ... first node ... instructions ... decoding ...encoded message ...", as broadly interpreted by the examiner.]; and

providing the set of one or more instructions to the second node *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys for the subsequent data transfer, as a result of requesting to establish a chat channel, and, whereas the key generation knows to 'whom' it must establish a decoding key (i.e., the 1st and 2nd chat participant identities was known to the key generating element, for the keys (i.e., instructions) to have been subsequently sent), clearly encompasses the "...providing ... instructions ... second node ...", as broadly interpreted by the examiner.]*;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message contained in the set of one or more instructions by:

retrieving the key, and

decoding the encoded message using the key *[figures 4-7 and associated descriptions, as broadly interpreted by the examiner.]*.".

Further, as per claim 21, this claim is the embodied software claim for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection, as such; "A computer-readable medium for controlling access to a message that is communicated from a first node to a second node in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

generating, at the first node,

an encoded message by encoding the message with a key;

generating, at the first node,

a set of one or more instructions that contain

the encoded message and

instructions for decoding the encoded message using the key; and

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message contained in the set of one or more instructions by:

retrieving the key, and

decoding the encoded message using the key to recover the original message.".

Further, as per claim 26, this claim is the apparatus claim for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection, as such; "A computer system comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

generating, at the first node,

an encoded message by encoding the message with a key;

generating, at the first node,

a set of one or more instructions that contain

the encoded message and

instructions for decoding the encoded message using the key; and

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the message to be recovered from the encoded message contained in the set of one or more instructions by:

retrieving the key, and

decoding the encoded message using the key to recover the original message.".

Further, as per claim 17, this claim is the broader claim in that the encoded message does not, at the very least, first require an identifier from the second node prior to encoding, as specifically designated from originating at the second node for the method claim 1 above, insofar as the key deletion aspect of the claim is concerned, and is rejected for the same reasons provided for the claim 1 rejection, as such; "The method as recited in Claim 16, further comprising

deleting the retrieved key *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys, subsequently transferring data, and the channel status monitor section (i.e., figure 7) generating another replacement secret key (i.e., inherently deleting the effective chat data transfer key, in of itself a function of a policy per*

se that is an operational characteristic of the chat system), clearly encompasses the "...deleting ... key", as broadly interpreted by the examiner.].".

Further, as per claim 22, this claim is the embodied software claim for the method claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection, as such; "The computer-readable medium as recited in Claim 21, further carrying one or more additional sequences of one or instructions which, when executed by the one or more processors, causes the one or more processors to perform the additional step of

deleting the retrieved key.".

Further, as per claim 27, this claim is the apparatus claim for the method claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection, as such; "The computer system as recited in Claim 26, wherein the memory further carries one or more additional sequences of one or instructions which, when executed by the one or more processors, causes the one or more processors to perform the additional step of deleting the retrieved key.".

10. Claim 20 ***additionally recites*** the limitation that; "The method as recited in Claim 16, wherein

the set of one or more instructions includes

address data that indicates a location from which the key may be retrieved.".

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network having had received secret

keys for the subsequent data transfer, such that the encoding/decoding can properly occur, is inherently an indication that encoding/decoding were provided the same ID, key, etc., and were communicated across the network to the appropriate node address (i.e., identification of location or address), clearly encompasses the "... instructions ... address data ...location ...", as broadly interpreted by the examiner.).

Further, as per claim 25, this claim is the apparatus claim for the method claim 20 above, and is rejected for the same reasons provided for the claim 20 rejection, as such; "The computer-readable medium as recited in Claim 21, wherein

the set of one or more instructions include

address data that indicates a location from which the key may be retrieved. ".

Further, as per claim 30, this claim is the apparatus claim for the method claim 20 above, and is rejected for the same reasons provided for the claim 20 rejection, as such; "The computer system as recited in Claim 26, wherein

the set of one or more instructions include

address data that indicates a location from which the key may be retrieved.".

11. As per claim 31; "A method for controlling access to a message that is communicated from a first node to a second node in a network, the method comprising the computer-implemented steps of:

generating, at the first node,

an encoded message by encoding the message with a key *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys (i.e., inherently generated per se in order to have been transferred) for the subsequent data transfer (i.e., the chat content data, post message encoding), as a result of requesting to establish a chat channel, clearly encompasses the "... generating ... first node ... encoded message ... key ...", as broadly interpreted by the examiner.]*;

generating, at the first node,

a set of one or more instructions that contain

the encoded message and

instructions for transferring to a third node the encoded message and instructions for retrieving the key *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys (i.e., inherently generated and identified as part of the 2 chat participating nodes identity per se in order to have been transferred) for the subsequent data transfer (i.e., the chat content data, post message encoding), as a result of requesting to establish a chat channel, and, whereas the key generation knows (i.e., the third node) to 'whom' it must establish a decoding key (i.e., the 1st chat participant identity must be made known to the key generating element), clearly encompasses the "... generating ... first node ... instructions ... third node ...encoded message ...", as broadly interpreted by the examiner.]*;

providing the set of one or more instructions to the second node *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys for the subsequent data transfer, as a result of requesting to establish a chat channel, and, whereas the key generation knows to 'whom' it must establish a decoding key (i.e., the 1st and 2nd chat participant identities was known to the key generating element, for the keys (i.e., instructions) to have been subsequently sent), clearly encompasses the "...providing ... instructions ... second node ...", as broadly interpreted by the examiner.]*;

wherein, processing the set of one or more instructions at the second node causes

the encoded message and

the instructions for retrieving the key to be transferred to the third node *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys for the subsequent data transfer, as a result of requesting to establish a chat channel, and, whereas the key generation knows to 'whom' it must establish a decoding key (i.e., the 1st and 2nd chat participant identities was known to the key generating element, for the keys (i.e., instructions) to have been subsequently sent), clearly encompasses the "...instructions at the second node ... instructions for retrieving the key ... third node ...", as broadly interpreted by the examiner.]*; and

wherein, the receiving, at the third node, of

the encoded message and

the instructions for retrieving the key causes:

the message to be recovered from the encoded message by

retrieving the key, and

decoding the encoded message using

the key, and

the recovered message to be provided from

the third node to

the second node *[figures 4-7 and associated descriptions, as broadly interpreted by the examiner.]*.".

Further, as per claim 37, this claim is the embodied software claim for the method claim 31 above, and is rejected for the same reasons provided for the claim 31 rejection, as such; "A computer-readable medium for controlling access to a message that is communicated from a first node to a second node in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key;

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third node, of the encoded message and the instructions for retrieving the key causes: the message to be recovered from the encoded message by retrieving the key, and decoding the encoded message using the key, and the recovered message to be provided from the third node to the second node.".

Further, as per claim 43, this claim is the apparatus claim for the method claim 31 above, and is rejected for the same reasons provided for the claim 31 rejection, as such; "A computer system for controlling access to a message that is communicated from a first node to a second node in a network, the computer system comprising:

one or more processors; and

a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, causes the one or more processors to perform the steps of:

generating, at the first node, an encoded message by encoding the message with a key;

generating, at the first node, a set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key;

providing the set of one or more instructions to the second node;

wherein, processing the set of one or more instructions at the second node causes the encoded message and the instructions for retrieving the key to be transferred to the third node; and

wherein, the receiving, at the third mode, of the encoded message and the instructions for retrieving the key causes: the message to be recovered from the encoded message by retrieving the key, and decoding the encoded message using the key, and the recovered message to be provided from the third node to the second node.".

12. Claim 32 ***additionally recites*** the limitation that; "The method as recited in Claim 31, wherein

the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further causes

the key to be deleted from the third node after the encoded message is decoded.". The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network receiving secret keys, subsequently transferring data, and the channel status monitor section (i.e., figure 7) generating another replacement secret key (i.e., inherently deleting the effective chat data transfer key, in of itself a function of a policy per se that is an operational characteristic of the chat system), clearly encompasses the "...deleting ... key", as broadly interpreted by the examiner.).

Further, as per claim 38, this claim is the embodied software claim for the method claim 32 above, and is rejected for the same reasons provided for the claim 32 rejection, as such; "The computer-readable medium as recited in Claim 37, wherein

the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further causes

the key to be deleted from the third node after the encoded message is decoded.".

Further, as per claim 44, this claim is the apparatus claim for the method claim 32 above, and is rejected for the same reasons provided for the claim 32 rejection, as such; "The computer system as recited in Claim 43, wherein the receiving, at the third node, of the encoded message and the instructions for retrieving the key, further causes the key to be deleted from the third node after they encoded message is decoded.

13. Claim 33 ***additionally recites*** the limitation that; "The method as recited in Claim 31, wherein

the set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key comprises

an HTML document.".

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the packet transfer nature of the Internet WWW (of

which HTML documents are an inherent part of the communications protocol), consisting of data fragments, clearly encompasses the "... instructions ... message ... key ... HTML document", as broadly interpreted by the examiner.).

Further, as per claim 39, this claim is the embodied software claim for the method claim 33 above, and is rejected for the same reasons provided for the claim 33 rejection, as such; "The computer-readable medium as recited in Claim 37, wherein

the set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key comprises

an HTML document.".

Further, as per claim 45, this claim is the apparatus claim for the method claim 33 above, and is rejected for the same reasons provided for the claim 33 rejection, as such; "The computer system as recited in Claim 43, wherein the set of one or more instructions that contain the encoded message and instructions for transferring to a third node the encoded message and instructions for retrieving the key comprises an HTML document.".

14. Claim 36 ***additionally recites*** the limitation that; "The method as recited in Claim 35, wherein

the URL query parameters also contain

control information, which

specifies

the order and

number of message fragments, and

enables the third node to

reconstruct the complete message.".

The teachings of Matsumoto are directed towards such limitations (i.e., figures 1-6 and associated descriptions, abstract, gggggg, whereas hhhhhh, clearly encompasses the "... jjjjjj ...", as broadly interpreted by the examiner.).

Further, as per claim 42, this claim is the embodied software claim for the method claim 36 above, and is rejected for the same reasons provided for the claim 36 rejection, as such; "The computer-readable medium as recited in Claim 41, wherein

the URL query parameters also contain

control information, which

specifies

the order and

number of message fragments, and

enables the third node to

reconstruct the complete message.".

Further, as per claim 48, this claim is the apparatus claim for the method claim 36 above, and is rejected for the same reasons provided for the claim 36 rejection, as such; "The computer

system as recited in Claim 47, wherein the URL query parameters also contain control information, which specifies the order and number of message fragments, and enables the third node to reconstruct the complete message.

15. As per claim 49; "A method for exchanging data between nodes in a network, the method comprising the computer-implemented steps of:

splitting the data into

two or more data fragments *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the packet transfer nature of the Internet consisting of data fragments, clearly encompasses the "...splitting the data ... data fragments ...", as broadly interpreted by the examiner.]*;

embedding

control information and

each data fragment from the two or more data fragments in a URL *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the inherent packet disassembly /re-assembly and associated transfer, and associated routing (Internet stack and flow control, and via Web links) nature of the Internet; consisting of data fragments, clearly encompasses the "... Embedding ... control information ...data fragments ... URL ...", as broadly interpreted by the examiner.]*;

providing the URLs from

a source node to

a destination node *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the inherent packet disassembly /re-assembly and associated transfer (i.e., data packets with associated higher level protocol structures such as the URL links, etc.,), and associated routing nature of the Internet; consisting of data fragments, clearly encompasses the "...providing the URLs from ... source node ... destination node", as broadly interpreted by the examiner.]*; and

wherein

the two or more data fragments and

control information may be extracted from the URLs at

the destination node *[figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the inherent packet disassembly /re-assembly (i.e., the extraction at the destination) and associated transfer (i.e., data packets with associated higher level protocol structures such as the URL links, etc.,), and associated routing nature of the Internet; consisting of data fragments, clearly encompasses the "...providing the URLs from ... source node ... destination node", as broadly interpreted by the examiner.]*.";

Further, as per claim 55, this claim is the embodied software claim for the method claim 49 above, and is rejected for the same reasons provided for the claim 49 rejection, as such; "A

computer-readable medium for exchanging data between nodes in a network, the computer-readable medium carrying one or more sequences of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of: splitting the data into two or more data fragments; embedding control information and each data fragment from the two or more data fragments in a URL; providing the URLs from a source node to a destination node; wherein the two or more data fragments and control information may be extracted from the URLs at the destination node.";

Further, as per claim 61, this claim is the apparatus claim for the method claim 49 above, and is rejected for the same reasons provided for the claim 49 rejection, as such; "A computer system comprising: one or more processors; and a memory communicatively coupled to the one or more processors and carrying one or more sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of: splitting the data into two or more data fragments: embedding control information and each data fragment from the two or more data fragments in a URL: providing the URLs from a source node to a destination node; wherein the two or more data fragments and control information may be extracted from the URLs at the destination node.".

16. Claim 50 ***additionally recites*** the limitation that; "The method as recited in Claim 49, wherein

the URLs are provided from

the source node to

the destination node using the HTTP protocol.".

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the packet transfer nature of the Internet WWW (of which HTML documents and packet disassembly (at the source; specifying a destination)/re-assembly (at the destination; as so specified to have arrived at the said destination) are an inherent part of the implementation of the HTTP communications protocol) and associated transfer (i.e., data packets with associated higher level protocol structures such as the URL links, etc.,), and associated routing nature of the Internet; consisting of data fragments, clearly encompasses the "...URLs are provided ... source node ... destination node ... HTTP protocol", as broadly interpreted by the examiner.).

Further, as per claim 56, this claim is the embodied software claim for the method claim 50 above, and is rejected for the same reasons provided for the claim 50 rejection, as such; "The computer-readable medium as recited in Claim 55, wherein the URLs are provided from the source node to the destination node using the HTTP protocol.".

Further, as per claim 62, this claim is the apparatus claim for the method claim 50 above, and is rejected for the same reasons provided for the claim 50 rejection, as such; "The computer system as recited in Claim 61, wherein the URLs are provided from the source node to the destination node using the HTTP protocol.".

17. Claim 51 ***additionally recites*** the limitation that; "The method as recited in Claim 50, wherein

the URLs are contained within

an HTML document.".

The teachings of Matsumoto are directed towards such limitations (figures 4-7 and associated descriptions, whereas the individual chat clients on the chat network of which the Internet is taught to be one embodied network of which the packet transfer nature of the Internet WWW (of which HTML documents and packet disassembly (at the source; specifying a destination)/re-assembly (at the destination; as so specified to have arrived at the said destination) are an inherent part of the implementation of the HTTP communications protocol) and associated transfer (i.e., data packets with associated higher level protocol structures such as the URL links, etc.,), and associated routing nature of the Internet; consisting of data fragments, clearly encompasses the "...URLs are contained ... HTML document", as broadly interpreted by the examiner.).

Further, as per claim 57, this claim is the embodied software claim for the method claim 51 above, and is rejected for the same reasons provided for the claim 51 rejection, as such; "The computer-readable medium as recited in Claim 56, wherein the URLs are contained within an HTML document.".

Further, as per claim 63, this claim is the apparatus claim for the method claim 51 above, and is rejected for the same reasons provided for the claim 51 rejection, as such; "The computer system as recited in Claim 62, wherein the URLs are contained within an HTML document.".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 18,19,23,24,28,29,34,35,40,41,46,47,52-54,58-60,64-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto, U.S. Patent 6,215,877 B1 as applied to claims 16,21,26,31,37,43,49,55,61 above, and further in view of Gupta et al, U.S. Patent 6,226,752 B1.

18. As per claim 18; "The method as recited in Claim 16, wherein
the set of one or more instructions comprises
a set of Javascript instructions.".

Further, as per claim 23, this claim is the apparatus claim for the method claim 18 above, and is rejected for the same reasons provided for the claim 18 rejection, as such; "The computer-readable medium as recited in Claim 21, wherein
the set of one or more instructions comprises

a set of Javascript instructions.".

Further, as per claim 28, this claim is the apparatus claim for the method claim 18 above, and is rejected for the same reasons provided for the claim 18 rejection, as such; "The computer system as recited in Claim 26, wherein

the set of one or more instructions comprises

a set of Javascript instructions.".

19. Claim 19 ***additionally recites*** the limitation that; "The method as recited in Claim 16, wherein

the set of one or more instructions comprises

a set of Java applet instructions.".

Further, as per claim 24, this claim is the apparatus claim for the method claim 19 above, and is rejected for the same reasons provided for the claim 19 rejection, as such; "The computer-readable medium as recited in Claim 21, wherein

the set of one or more instructions comprises

a set of Java applet instructions.".

Further, as per claim 29, this claim is the apparatus claim for the method claim 19 above, and is rejected for the same reasons provided for the claim 19 rejection, as such; "The computer system as recited in Claim 26, wherein

the set of one or more instructions comprises

a set of Java applet instructions.".

20. Claim 34 ***additionally recites*** the limitation that; "The method as recited in Claim 33, wherein

the HTML document comprises

an HTML form with fields containing

the encoded message and

key address data,

a submit button to

submit the form to the third node, and

JavaScript to

automatically submit the form to the third node.".

Further, as per claim 40, this claim is the embodied software claim for the method claim 34 above, and is rejected for the same reasons provided for the claim 34 rejection, as such; "The computer-readable medium as recited in Claim 39, wherein

the HTML document comprises

an HTML form with fields containing

the encoded message and

key address data,

a submit button to

submit the form to the third node, and

JavaScript to

automatically submit the form to the third node.".

Further, as per claim 46, this claim is the apparatus claim for the method claim 34 above, and is rejected for the same reasons provided for the claim 34 rejection, as such; "The computer system as recited in Claim 45, wherein the HTML document comprises an HTML form with fields containing the encoded message and key address data, a submit button to submit the form to the third node, and JavaScript to automatically submit the form to the third node.".

21. Claim 35 ***additionally recites*** the limitation that; "The method as recited in Claim 33, wherein

the HTML document comprises

a set of associated URLs embedded in multiple

<img>,

<ilayer>,

<applet>, or

<iframe> elements,

wherein each URL contains

fragments of the encoded message and

key address data as URL query parameters, and

wherein each URL specifies

the location of the third node.".

Further, as per claim 41, this claim is the embodied software claim for the method claim 35 above, and is rejected for the same reasons provided for the claim 35 rejection, as such; "The computer.-readable medium as recited in Claim 39, wherein

the HTML document comprises

a set of associated URLs embedded in multiple

<imp>,

<ilayer>,

<applet>, or

<iframe> elements,

wherein each URL contains fragments of

the encoded message and

key address data as URL query parameters, and

wherein each URL specifies

the location of the third node.".

Further, as per claim 47, this claim is the apparatus claim for the method claim 35 above, and is rejected for the same reasons provided for the claim 35 rejection, as such; "The computer system as recited in Claim 45, wherein the HTML document comprises a set of associated URLs embedded in multiple <img>, <ilayer>, <applet>, or <iframe> elements, wherein each URL

contains fragments of the encoded message and key address data as URL query parameters, and wherein each URL specifies the location of the third node.".

22. Claim 52 ***additionally recites*** the limitation that; "The method as recited in Claim 51, wherein

each URL contained within the HTML document, is

embedded in an

<img>,

<ilayer>,

<applet>, or

<iframe> element,

contains fragments of

the data as URL query parameters, and

specifies a location of

the destination node.".

Further, as per claim 58, this claim is the embodied software claim for the method claim 52 above, and is rejected for the same reasons provided for the claim 52 rejection, as such; "The computer-readable medium as recited in Claim 57, wherein each URL contained within the HTML document, is embedded in an <img>, <ilayer>, <applet>, or <iframe> element, contains fragments of the data as URL query parameters, and specifies a location of the destination node.".

Further, as per claim 64, this claim is the apparatus claim for the method claim 52 above, and is rejected for the same reasons provided for the claim 52 rejection, as such; "The computer system as recited in Claim 63, wherein each URL contained within the HTML document, is embedded in an <img>, <ilayer>, <applet>, or <iframe> element, contains fragments of the data as URL query parameters, and specifies a location of the destination node.".

23. Claim 53 ***additionally recites*** the limitation that; "The method as recited in Claim 52, wherein

the URL query parameters also contain

control information, which

specifies

an order and

number of data fragments to

enable the data to be reconstructed at

the destination node.".

Further, as per claim 59, this claim is the embodied software claim for the method claim 53 above, and is rejected for the same reasons provided for the claim 53 rejection, as such; "The computer-readable medium as recited in Claim 58, wherein the URL query parameters also contain control information, which specifies an order and number of data fragments to enable the data to be reconstructed at the destination node.".

Further, as per claim 65, this claim is the apparatus claim for the method claim 53 above, and is rejected for the same reasons provided for the claim 53 rejection, as such; "The computer system as recited in Claim 64, wherein the URL query parameters also contain control information, which specifies an order and number of data fragments to enable the data to be reconstructed at the destination node.".

24. Claim 54 ***additionally recites*** the limitation that; "The method as recited in Claim 53, wherein:

the HTML document is

embedded in a registration email received at

the source node,

the data fragments embedded in the URLs include

registration and

user information, and

the method further comprises the computer-implemented steps of:

providing the data to

the destination node when

the registration email is read;

generating an authentication cookie on

the source node in response to receiving

the registration and

user information;

using the authentication cookie to authenticate a user at

the source node when the source node makes subsequent client requests to

the destination node.".

Further, as per claim 60, this claim is the embodied software claim for the method claim 54 above, and is rejected for the same reasons provided for the claim 54 rejection, as such; "The computer-readable medium as recited in Claim 59, wherein: the HTML document is embedded in a registration email received at the source node, the data fray embedded in the URLs include registration and user information, and the computer-readable medium further comprises one or more additional sequences of one or more instructions which, when executed by the one or more processors, causes the one or more processors to perform the computer-implemented steps of: providing the data to the destination node when the registration email is made; generating an authentication cookie on the source node in response to receiving the registration and user information; using the authentication cookie to authenticate a user at the source node when the source node makes subsequent client requests to the destination node.";

Further, as per claim 66, this claim is the apparatus claim for the method claim 54 above, and is rejected for the same reasons provided for the claim 54 rejection, as such; "The computer system as recited in Claim 65, wherein: the HTML document is embedded in a registration email received at the source node, the data fragments embedded in the include registration and user information, and the memory further comprises one or more additional sequences of one or more

instructions which, when executed by the one or more processors, causes the one or more processors to perform the computer-implemented steps of: providing the data to the destination node when the registration email is read; generating an authentication cookie on the source node in response to receiving the registration and user information; using the authentication cookie to authenticate a user at the source node when the source node makes subsequent client requests to the destination node.".

The teachings of Matsumoto suggest the base claims limitations (see "As per claim 16, ... As per claim 21, ...26, ...31, ...37, ...43, ...49, ...55, ...61" paragraphs above) *without explicitly teaching* of the use of the Internet WWW web page features/embedded elements (i.e., Java, Javascript, specific field within a web page embedded linking criteria, etc.,) for the chat node to chat node and key management server communications protocols.

Gupta et al, teaches of using a multiple node client / server message / user authentication / encryption method / apparatus that is, in multiple embodiments, implemented using various object oriented and more specifically, web based programming languages (i.e., Java and its associated variants and scripting derivatives; Gupta et al col. 8,lines 61-col. 14,line 64) and applications (i.e., email, browsing per se). The Gupta et al invention also clearly encompasses the security aspects associated with the applicants network message communications aspects (i.e., Gupta et al, figure 2 and associated descriptions).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Matsumoto network message communication, with the Gupta et al teachings of object oriented / web based programming and applications in

order to provide the WWW orientation of the generally Internet oriented Matsumoto network message communication invention.

Such motivation to combine would clearly encompass the need to allow comprehensive WWW aspects of the Internet based network communications in cryptographic oriented network communications (i.e., Gupta et al col. 1,lines 5-col. 6,line 51).

Claim Objections

28. Claim 12 ***additionally recites*** the limitation that; "The computer system as recited in Claim 11, wherein the memory further includes one or more additional sequences of one or more instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of: receiving a second request from the first node for a second message identifier that uniquely identifies a second message and a second key that may be used to encode the second message; generating, in response to the second request, both the second message identifier and the second key; providing both the second message identifier and the second key to the first node to allow the second message to be encoded with the second key to generate a second encoded message; receiving a second request from the second node for the second key; generating second algorithm identification data that indicates a second algorithm to be used to decode the second encoded message; providing the second algorithm identification data to the second node; providing the second key and the second identification data to the second node to allow the second encoded message to be decoded and the second message to be retrieved using the second key; and deleting the second key based upon the specified key policy criteria to prevent copies of the second encoded message from being decoded.";

Claim 12 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 11. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Applicant is further advised that for the sake of applying art, the examiner assumes that claim 12 is actually means plus function claims for the limitations of claim 11, (i.e., see; In re Donaldson, 16 F.3d 1189, 1193, 29 USPQ2d 1845, 1848 (Fed. Cir. 1994); see Kemco Sales, Inc. v. Control Papers Company, Inc., 208 F.3d 1352, 54 USPQ2d 1308 (Fed. Cir. 2000); see MPEP § 2181 through § 2186 in accordance with 35 U.S.C. 112, sixth paragraph and MPEP §2181 through § 2186).

Conclusion

26. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

6/10/05